

MODELLING MALICIOUS ENTITIES IN A ROBOTIC SWARM

Ian Sargeant and Allan Tomlinson

Information Security Group, Royal Holloway, University of London

Egham Hill, Egham. Surrey. TW20 0EX. U.K.

Abstract

Work has been undertaken in the research of swarm robotics and potential applications. This has included several specific models and simulations, with the majority of the work assuming a benign operational environment for the swarm. This paper proposes a generic model to represent a swarm and then adapts the generic model to consider malicious elements within the swarm.

Introduction

This paper proposes a model that enables the representation of both a swarm and malicious intruders within the swarm.

There has been a significant amount of research undertaken in to the proposed uses [1-3] and physical implementations of swarm robotics [4-8], along with the associated modelling [9-17] and simulation techniques [18-22]. However, to date, none of the models or simulations appears to have considered security implications for a swarm. That is, due to the relative infancy of swarm robotics the proposed uses. Models and simulations assume trust of the interacting swarm elements as a pre-requisite condition and the current physical implementations have been implemented in relatively benign conditions. Our concern, however, is with swarms that might operate in hostile environments.

This paper proposes a generic model for a swarm and introduces the concepts of both the modelling of failed swarm elements and the modelling of a malicious intruder within the swarm. This paper will highlight the differences between a failed element and a malicious intruder and allow a greater understanding of the concepts and representation within a model.

To assist in the understanding of the proposed model and place the model in context, an overview is provided on the concept of swarms and the concept of security within a swarm, focusing on an intruder within a swarm.

In order to understand the research question, it is important to have an understanding of a swarm. The research question can then be introduced within context.

Introduction To A Swarm

In order to understand the proposal, it is necessary to introduce and define what we mean by a swarm, in the context of this paper.

Swarm robotic research is looking at multi-robot systems and is currently taking the majority of its inspiration from nature [23]. The philosophy behind a robotic swarm is that a large number of relatively basic robots will work in conjunction with each other to complete a predetermined goal. It is generally agreed that a swarm has the following characteristics [24-34]:

- Autonomy
- Decentralised control
- Large number of members
- Collective emergent behaviour
- Local sensing
- Local communications
- Resilience to failures within the swarm

Indeed, [27] describes a swarm robotics as: "... the study of how large numbers of relatively simple physically embodied agents can be designed such that a desired collective behaviour emerges from the local interaction among agents and between agents and the environment."

Swarm robotics is generally within the research environment and actual applications for the use of swarm robotics are often theoretical. However, it is the proposed uses of swarms and the potential benefits that swarm robotics could deliver which is driving the majority of the research.

There are proposed applications of swarm robotics in both civilian and military applications.

Typical civilian applications include [2,3,35,36]:

- Maintenance tasks
- Communications provision
- Emergency Response:
 - Ad-hoc communications
 - Search and Rescue
 - Contaminant tracking
 - Initial and continuous disaster scene information
- Use in space flights and exploration
- Medical procedures

Typical military applications include [37-40]:

- Military communications
- Underwater mine clearance
- Landmine detection
- Situational Awareness

Introduction To The Problem

A swarm is an autonomous body operating, in many cases, beyond the control and visibility of the authority that launched it. However, it is not inconceivable that swarms may operate in hostile environments where an attacker may detect the swarm and attempt to manipulate its behaviour. The motivation of an attacker will vary, based on the objective of the swarm and the approach and mindset of an attacker. To place this into context, an airborne swarm has the objective of communications provision to ground forces, the attacker will want to disrupt the communications and therefore attempts to alter the behaviour of the swarm. Within the commercial environment, swarms might be used in mineral or oil exploration, a competitor might wish to either observe the swarm in order to gain information or reduce the swarm's efficiency to gain a competitive advantage. There is also an attacker group that will attempt to affect the swarm just simply for the challenge to prove it can be done, this is analogous to the defacement of websites.

The overarching problem is therefore to determine whether the expected behaviour of a swarm can be altered by an attacker, and if it can, then to what extent?

We suggest that there are several processes that could alter the behaviour of the swarm. Such as:

1. A swarm element fails – a non-malicious event
2. A rouge swarm element attacks the original swarm – a malicious event
3. Unexpected environmental events – could be both a non-malicious or a malicious action

Our intention is to develop a model that can be used to formally express this problem.

In order to develop a model we considered existing descriptions of swarms. Within the literature, many types of swarm schemes are described. Most of these can be categorised as belonging to one of three general types of model: models based on gas particles [41], models based on Newtonian physics [42] and models based on simple algorithms [43]. The aim of this paper is to propose an abstract generic model that can be applied to all these types of swarms. However, our main objective is to consider the inclusion of failed swarm elements and malicious elements.

Failed Element

As with any mechanical system, it might eventual succumb to failures.

To put this into the context in the natural world, if an ant dies, the remaining ants within a colony will continue to function as normal. Indeed, certain basic actions of the colony might temporarily change to removing the deceased ant, in order to preserve the health of the remaining colony inhabitants [23], and then return to the original undertaking.

Based on the implementation and goal of a swarm, the actions of the swarm would differ if failure occurs. That is, there could be significant differences in the swarm's behaviour depending on whether or not a swarm element was able to monitor and reports its own health. For example, if a swarm element suspected that it was failing, it could simply remove itself from the swarm, such as by stopping communications with other swarm elements, or increase separation distances to avoid collisions. The

actions of the remaining swarm elements would then continue as normal. There are proposals that would enable swarm elements to monitor their health and interact with other entities [36] where there is research being conducted in secondary swarms attempting to repair failed primary swarm elements.

The Malicious Intruder

It is proposed that the purpose of a malicious intruder within a swarm has the goal of either preventing the swarm from completing its original undertaking or has the goal of reducing the efficiency of the original swarm. This could be by slowing the original swarm in its undertaking or altering any emergent swarm behaviour. We are concerned with the malicious intruder in the swarm and will concentrate upon this. To place the malicious intruder into context, if a swarm was being deployed to search for and identify landmines the consequence of a delay would be different, depending upon the scenario. If the swarm were being utilised post conflict to assist in the removal of landmines for humanitarian reasons, the delay of a swarm could be observed and the main impact would be a delay in landmine clearance. If the swarm was released in front of advancing troops and the troops caught up with or overtook the swarm, the troops would be entering a minefield without any knowledge of the location of the landmines. The impact would be different in each circumstance, in that the impact would be either a time delay, during landmine clearance, as opposed to no protection to advancing troops.

The goal of the malicious intruder would be dependent upon the goal of the original swarm and therefore the proposed model for the malicious intruder is a generic model.

This does present the question that, from a swarm's perspective, what is the difference between a malicious intruder and a failed element, effectively acting as non-malicious intruder? This has been identified within the proposed models.

Unexpected Environmental Effects

By the very nature of the swarm, the swarm will interact with the environment. In fact, the use of stigmergy has been proposed as a communications method for certain swarm implementations [35].

An environmental effect could be as simple as a physical barrier either slowing down or preventing a ground moving swarm from moving in a desired direction, such as a ditch or a wall, or unexpected gusting winds blowing an airborne swarm off course. There could also be the effect of damage being caused to swarm elements, such as falling debris within disaster recovery, where the swarm elements communications still function but the ability to move has been prevented.

Therefore, the environment could have either significant or unexpected effects on a swarms behaviour or efficiency and could be either non-malicious or malicious in intent.

Overview Of Security Considerations

There are several considerations with regards security. As described in [44] the main aspects of security regarding a swarm are: Confidentiality, Integrity, Availability and Access Control.

Confidentiality

The requirement to protect information from authorised disclosure. Examples of this within a swarm this could be communications within a swarm or communications from the swarm. That is, an airborne swarm might have the task of locating an object, say a person. The communications to and within the swarm, prior to its release, would contain the location to search, which the swarm's controlling authority might wish to keep protected, and similarly if the swarm achieves its goal and finds the person, then the controlling authority might not wish this to be apparent to an external observer. There might also the potential requirement to protect information contained within a swarm element. That is, if a swarm element is captured, could an adversary obtain information from within the swarm element?

Integrity

The requirement to prevent data from being altered in an unauthorised or unintended way. An example of this within a swarm would be the communications between swarm elements and ensuring that the communications had not been altered so as to alter the behaviour of the swarm, such as making a swarm alter course.

Availability

The requirement for a system or data to be accessible and usable upon demand by an authorised entity. The term Denial of Service is often used to describe a loss of availability. Again, communications between swarm elements provides a good example of how availability can be affected between elements within a swarm. If an adversary were to interfere with the communications, such as by jamming, it might be possible to prevent the swarm from functioning, effectively a denial of service to the swarm, or the attacker might be able to prevent the swarm from passing information back to a controlling authority. That is, say the swarm was looking for an enemy soldier, and it finds one but the enemy manages to prevent the swarm from communicating this information, then the availability of this information has been prevented. Essentially the swarm is functioning but it cannot communicate to an external entity.

Access Control

The requirement to allow only authorised access to a system. This will generally comprise of a form of Identification and Authentication to permit authorisation to a system and may include various levels of access, based on the provided details. This could be difficult to implement within a swarm, due to the homogeneous nature of a swarm. However, a form of group identification might be used to prevent members from other swarms from joining or affecting the original swarm.

Modelling the Swarm

The following generic models have been proposed, in order to model the various instances of swarms and swarm elements.

Initial Swarm Definition

The initial swarm is defined as a large number of entities that have attributes and will exhibit actions based on interactions with other swarm entities and the environment [27].

The swarm is defined as a set of entities S , such that:

$$S = \{s_0, s_1, \dots, s_n\}$$

where n is the number of entities within the swarm and each swarm entity, s_x , has the same specific attributes.

It should be noted that the attributes of a swarm entity, s_x , are not necessarily the same attributes as the overall swarm itself, S . This model also allows for consideration of similar properties, which could be confused. A typical example of this could be a time goal. That is, one of the swarm's goals could be to arrive at a location by a particular time. However, the swarm elements might have the goal to arrive at a location in the most efficient manner that can be perceived by the swarm elements, as deduced by the "swarm's intelligence" [23,37,38,45-49]. However, the swarm, S , might not be able to arrive at the location by the required time, such as due to environmental effects, but will arrive there eventually. Therefore, both the swarm goal and the swarm elements goal are related to time, but have different contexts.

The attributes will be specific to the design of the swarm and will contain information that allows the swarm to operate. Typical examples of attributes could be:

- Location
- Velocity
- Time

The swarm itself may have certain attributes that relate to the goal of the swarm and therefore this paper assumes that a goal of a swarm can be an attribute of a swarm.

It is also worth noting that different swarms may interpret the attributes based on the particular design. That is, a location attribute might be a latitude and longitude measurement, or it might be distances relative to an arbitrary point or datum. Similarly, time could be based on the Universal Time Constant (UTC) or seconds elapsed since the swarm was released.

The attributes for the overall swarm S are defined by a tuple:

$$\langle sa_0, sa_1, \dots, sa_z \rangle$$

where sa is an attribute of a swarm and z is the number of attributes specific to the swarm.

The attributes for a swarm element, s_x , are defined by the tuple:

$$\langle a_0, a_1, \dots, a_y \rangle$$

where a is an attribute of a swarm entity and y is the number of attributes specific to the swarm entity.

Modelling a Failed Swarm Entity

It is entirely possible that swarm entities can fail, this can be due to such things as either mechanical failure or an external influence damaging a swarm entity.

There is a general understanding within the literature [24,50] that as a swarm is large enough, such perturbations can be ignored. In fact, an inherent redundancy and resilience within a swarm is often stated as one of the major beneficial factors regarding the use of a swarm.

Essentially, there is an argument that, due to the size of a swarm, a failed entity will have a negligible effect upon the remaining swarm members. This argument might be further enhanced by the fact that a swarm member has a limited range of observation, interaction and influence.

It is proposed that failed swarm entities form a subset, SF , of the original swarm, S , such that :

$$SF = \{sf_0, sf_1, \dots, sf_h\} \subset S$$

where h is the number of failed entities within the original swarm, this can be seen in Figure 1.

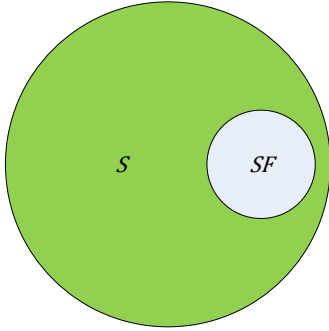


Figure 1. Initial and Failed Swarm Elements

In other words, since sf_x is a failed entity from the swarm S , it will have the same attributes as S , although they might have been affected in some way.

That is:

$$\langle a_0, a_1, \dots, a_y \rangle = \langle b_0, b_1, \dots, b_y \rangle$$

where a is the attribute of a normal/healthy swarm entity and b is attribute of a failed swarm entity.

Although there are the same attributes for each swarm, the values might have been altered such that

they are no longer characteristic of the original swarm in a normal mode of operation.

For instance, the swarm might have been heading in a certain direction at a predefined velocity. A failed entity might still have an attribute that accurately represents its location. However, its velocity attribute might be set to zero, based on a failure mode that prevents the entity from moving. Although this is a valid state, i.e. its velocity is zero; this might not be a normal state, based on the current emergent behaviour of the unaffected entities within the original swarm.

Modelling a Malicious Swarm

We define a malicious swarm as a number of elements that will attempt to effect the behaviour, or performance, of the original swarm.

Although the malicious swarm will have a goal, it does not necessarily have to be the same as the original swarm. That is, the original swarm might have the goal of clearing a minefield and the malicious swarm will have the goal of attempting to prevent this from happening, or the original swarm might have a goal to travel to a specific location and the malicious swarm might either prevent this from happening or slow the original swarm down, in order to effect the efficiency of the original swarm.

The malicious swarm is defined as a set of entities S' , such that:

$$S' = \{s'_0, s'_1, \dots, s'_m\}$$

where m is the number of malicious entities within the malicious swarm.

In a similar fashion to the original swarm, the malicious swarm has a number of attributes. The attributes for a malicious swarm entity, s'_x , are defined by the tuple:

$$\langle c_0, c_1, \dots, c_j \rangle$$

where c is an attribute of the malicious swarm entity and j is the number of attributes specific to the malicious swarm entity. Moreover, S' will have a different set of attributes:

$$\langle ca_0, ca_1, \dots, ca_w \rangle$$

where ca is an attribute of the malicious swarm and w is the number of attributes specific to the malicious swarm.

The quantity of the attributes of a malicious swarm entity can be either less than, equal to, or greater than the original swarm, which will be dependent upon the malicious swarm's design. Both swarms could have the same attributes but set to different values. For example, both the original swarm and the malicious swarm could have a maximum velocity limit. However, the malicious swarm might have a greater velocity limit, in order to be able to catch and affect the swarm.

It is also possible for an attacker to capture and modify an original swarm entity, in which case the attributes of the original swarm and the malicious swarm would be the same, although the original swarm attribute values may have been modified to allow the malicious swarm to undertake an attack. An example of an attribute that could be modified might include time allowed on task, where the original swarm might have a predefined time on task, in order to allow it to return to a location before its energy is depleted. The malicious swarm might ignore this attribute and just keep working until it fails, in order to attempt to affect the original swarm. If the modified swarm element were able to influence the time on task permitted for an original, unmodified swarm element, then this would be an example of a denial of service attack on availability, as discussed in Overview Of Security Considerations section regarding Availability.

Modelling Swarm Interaction

The assumption is that all the swarm types, S , SF and S' , will share common attributes, such as location and velocity.

To assist with understanding, the common attributes between an original swarm, S' , and a malicious swarm, S' , are examined.

This can be seen in Figure 2, where S and S' share certain attributes.

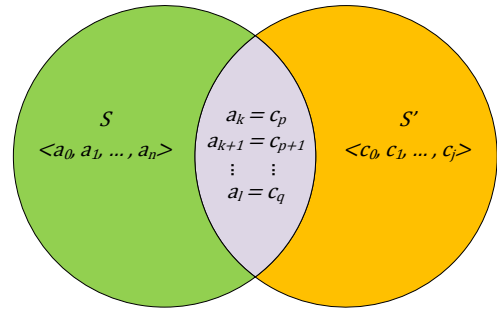


Figure 2. Initial & Malicious Swarm Relationship

The common attributes are shown in union $S \cup S'$ of the diagram are:

$$\langle a_k, a_{k+1}, \dots, a_l \rangle = \langle c_p, c_{p+1}, \dots, c_q \rangle$$

The aim of the malicious swarm, S' , is to alter the behaviour of the swarm, S , in the most efficient manner. This could be by the malicious swarm utilising as many common attributes as possible in order to affect the original swarm, or by utilising common attributes that have the greatest effect.

Another consideration is the size of malicious swarm that is required to alter the behaviour of the original swarm. The ideal requirement for the malicious swarm would be that the malicious swarm is significantly smaller than the original swarm.

Application

Landmine Example

In the following example, the goal of a swarm is attempting to locate, and then make safe, landmines within a given area [37-39]. The goal of the malicious swarm is to attempt to make the discovery of landmines an inefficient process.

Therefore, the swarm attempting to locate the landmines, with say 500 members, can be shown as:

$$S = \{s_0, s_1, \dots, s_{499}\}$$

This swarm, S , attempts to locate and make safe landmines by conducting a search. The attributes for the overall swarm,

$$\langle sa_0, sa_1, \dots, sa_z \rangle$$

Which could be: Search for landmines, make safe landmines, undertake within a particular time period.

The individual swarm entities, s_x , could have the following attributes:

$$\langle a_0, a_1, \dots, a_y \rangle$$

Which could be: location, current velocity, maximum velocity, maximum communications range, health of swarm element and power level.

As the swarm elements are mechanical, there might be occasions when elements of the original swarm, S , fail. Suppose 5 elements fail, this would generate a group of failed swarm elements, SF , such that:

$$SF = \{sf_0, sf_1, \dots, sf_4\} \subset S$$

As described earlier, the failed elements sf_x will have the same attributes as s_x . That is:

$$\langle a_0, a_1, \dots, a_y \rangle = \langle b_0, b_1, \dots, b_y \rangle$$

where a is the attribute of a normal/healthy swarm entity and b is attribute of a failed swarm entity.

Prior research has been undertaken on the effects of a failed swarm element [24, 28] and SF has been included here for completeness. The remainder of this paper will focus upon an attack by a malicious swarm, S' .

In this example the goal of S' is to alter the behaviour of the swarm, S , in the most efficient manner, such that S will either fail or reduce the efficiency of its original goal to find and make safe the landmines. That is, the goals of S and S' differ in that the goal of S is attempting to locate and make safe landmines, whereas the goal of S' to prevent S from undertaking this task.

The malicious swarm, containing say 100 elements, is defined as a set of entities S' , such that:

$$S' = \{s'_0, s'_1, \dots, s'_{99}\}$$

where 100 malicious entities are introduced within the malicious swarm.

In a similar fashion to the original swarm, the malicious swarm has a number of attributes. The attributes for a malicious swarm entity are defined by the tuple:

$$\langle c_0, c_1, \dots, c_j \rangle$$

There could be common attributes between s_x and s'_x , such as: location, current velocity, maximum velocity, maximum communications

range, etc. However, the values could be different, that is, s'_x could have a greater communications range, in order to influence S , and it might have a greater maximum velocity, in order to be able to infiltrate S as efficiently as possible. Certain attributes between s_x and s'_x will be different, S' will not want to detect mines but will want to prevent S from undertaking this, therefore s'_x might not care about its power level, as it has no reason to remove itself from the minefield.

Hunting Example

In some applications it is proposed that there is a requirement for a swarm to hunt out and find a target object over an efficient path, by using efficient navigation and shortest paths.

In this example, the swarm, S , attempts to find a target, T . The swarm elements, s_x , utilise the attributes distance to target and age of information data. A malicious swarm, S' , could attempt to make the process of locating T less efficient.

The malicious swarm elements, s'_x , could well have exactly the same attributes as s_x but modify the communicated values, in order to affect the overall efficiency of S . That is:

$$\langle a_0, a_1, \dots, a_y \rangle = \langle c_0, c_1, \dots, c_y \rangle$$

However, $\langle c_0, c_1, \dots, c_y \rangle$ report false data.

Communications Example

There are proposals to utilise swarms to provide communications bearers for external users.

Therefore, the goal of the swarm, S , would be to provide reliable communication. The goal of the malicious swarm, S' , is to either prevent or degrade the communications provision. In this example, the attributes of s'_x could be both the same as s_x , such as current velocity and location information, as well as different attributes, such as jamming power levels.

Review of Examples

To assist in understanding, the examples are summarised in Table 1 and Table 2, and the attributes of the various swarm elements, as defined in section Modelling the Swarm, are described.

Table 1. Original & Malicious Attributes

| | Mines | Hunting | Comms |
|------|---|----------------------------------|-----------------------------------|
| S | Locate Landmines. Make Landmines Safe. | Find/Locate Targets. | Provision Of Reliable Comms. |
| S' | Hinder And Prevent Landmine Location. | Increase Time To Locate Targets. | Disrupt, Prevent And Break Comms. |

Table 2. Typical Swarm Element Attributes

| | Mines | Hunting | Comms |
|--|------------------------------------|---|---|
| $\langle a_0, a_1, \dots, a_y \rangle$ | Location. Power. Velocity. | Distance to target. Age of information. | Location. Velocity. |
| $\langle b_0, b_1, \dots, b_y \rangle$ | Location. Power. Velocity. | Distance to target. Age of information. | Location. Velocity. |
| $\langle c_0, c_1, \dots, c_q \rangle$ | Location. Power. 2*Velocity. | Random distance to target. Lower age of information. | Location. 2 * Velocity. Jamming Energy |

As can be seen in all the examples provided, the attributes of a healthy swarm element s_x , $\langle a_0, a_1, \dots, a_y \rangle$, are the same as the attributes for a failed swarm element sf_x , $\langle b_0, b_1, \dots, b_y \rangle$. However, the attributes for a malicious swarm element s'_x , $\langle c_0, c_1, \dots, c_q \rangle$, can be either the same, modified or different. Thus, we can see from Table 2 how the proposed model can be applied to a variety of applications. This can then be used to identify attributes that might attack S .

Conclusion

In conclusion, this paper provides a generic model that allows the researcher to consider how a swarm, a swarm with failed elements and a malicious swarm can be modelled and identifies how various swarm attributes could be manipulated to cause an effect. The paper suggests how an external hostile swarm, specifically with a malicious intent, could affect an original swarm and how this could be modelled. The aim of this paper was to propose a generic model, to allow follow on work that would attempt to prove the model. However, the techniques to develop the proofs depend upon swarms' goals and particular implementations. Examples include particle physics, graph theory and Newtonian Physics. It is beyond the scope of this paper to propose a general mathematical proof that the swarm will meet a goal, especially with various ways a malicious intruder could affect an original swarm. The authors are continuing their research, based on this paper, by simulating various swarms with a view

to gaining an understanding, by examination of simulation results, as to what extent a malicious intruder can affect an original swarm. It is proposed to then follow this work with how to detect and mitigate such attacks.

References

- [1] Paul Scerri et al., A Prototype Infrastructure for Distributed Robot-Agent-Person Teams, 2003.
- [2] S. Subchan, B.A. White, A. Tsourdos, M. Shanmugavel, and R. Zbikowski, "Pythagorean Hodograph (PH) Path Planning for Tracking Airborne Contaminant using Sensor Swarm," in Instrumentation and Measurement Technology Conference Proceedings, 2008. IMTC 2008. IEEE, 2008, pp. 501-506.
- [3] H. Woern, M. Szymanski, and J. Seyfried, "The I-SWARM Project," in Robot and Human Interactive Communication, 2006. ROMAN 2006. The 15th IEEE International Symposium on, 2006, pp. 492-496.
- [4] Alcherio Martinoli, Kjerstin Easton, and William Agassounon, "Modeling Swarm Robotic Systems: a Case Study in Collaborative Distributed Manipulation," Int. Journal of Robotics Research, vol. 23, pp. 415-436, 2004. [Online]. http://www.kjerstin.com/pubs/04_AMKEWA_IJRR.pdf
- [5] Jakob Fredslund and Maja J Mataric, A General Algorithm for Robot Formations Using Local Sensing and Minimal Communication, 2002.
- [6] Tucker Balch and Ronald C. Arkin, "Behavior-based Formation Control for Multi-robot Teams," IEEE Transactions on Robotics and Automation, vol. 14, pp. 926-939, 1997. [Online]. <http://www.cc.gatech.edu/ai/robot-lab/online-publications/formjour.pdf>
- [7] Christopher M. Ciani, Xavier Raemy, Jim Pugh, Alcherio Martinoli, and Ecole Polytechnique Federale de Lausanne, "Communication in a Swarm of Miniature Robots: The e-Puck as an Educational Tool for Swarm Robotics," in Simulation of Adaptive Behavior (SAB-2006), Swarm Robotics Workshop, 2006, pp. 103-115. [Online]. <http://infoscience.epfl.ch/record/100015/files/44330103.pdf>
- [8] Brian P. Gerkey and Maja J. Mataric, Sold!: Auction Methods for Multirobot Coordination, 2002.

- [9] Jeffrey L. Dohner, "A Guidance and Control Algorithm for Scent Tracking Micro-Robotic Vehicle Swarms," Sandia National Laboratories, Tech. rep. 1997.
- [10] Christoph Moeslinger, Thomas Schmickl, and Karl Crailsheim, A Minimalist Flocking Algorithm for Swarm Robots.
- [11] Heiko Hamann and Heinz Worn, A Framework of Space-Time Continuous Models for Algorithm Design in Swarm Robotics.
- [12] Jan Dyre Bjerknes, Alan Ft Winfield, Chris Melhuish, and Coldharbour Lane, "An analysis of emergent taxis in a wireless connected swarm of mobile robots," in In IEEE Swarm Intelligence Symposium, 2007, pp. 45-52. [Online]. http://www.ias.uwe.ac.uk/~a-winfie/Bjerknes_etalIEEEIS07.pdf
- [13] Sebastian von Mammen and Christian Jacob, "Evolutionary Swarm Design of Architectural Idea Models," in Proceedings of the 10th annual conference on Genetic and evolutionary computation, New York, NY, USA, 2008, pp. 143-150. [Online]. <http://doi.acm.org/10.1145/1389095.1389115>
- [14] Sebastian von Mammen, "Swarm Grammars: Modeling Computational Development through Highly Dynamic Complex Processes," University of Calgary, Ph.D. dissertation June 2009.
- [15] R. Brooks, "A Robust Layered Control System for a Mobile Robot," Robotics and Automation, IEEE Journal of, vol. 2, no. 1, pp. 14-23, mar 1986.
- [16] Toshio Fukuda, Go Iritani, Tsuyoshi Ueyama, and Fumihito Arai, "Optimization of Group Behavior on Cellular Robotic System in Dynamic Environment.," in ICRA, 1994, pp. 1027-1032. [Online]. <http://dblp.uni-trier.de/db/conf/icra/icra1994-2.html#FukudaIUA94>
- [17] J. P. Desai, J. P. Ostrowski, and V. Kumar, "Modeling and control of formations of nonholonomic mobile robots," Robotics and Automation, IEEE Transactions on, vol. 17, no. 6, pp. 905-908, 2001. [Online]. <http://dx.doi.org/10.1109/70.976023>
- [18] Spring Berman, Adam Halasz, Vijay Kumar, and Stephen Pratt, "Bio-Inspired Group Behaviors for the Deployment of a Swarm of Robots to Multiple Destinations," in in Proceedings of IEEE International Conference on Robotics and Automation (ICRA), 2007. [Online]. <http://www.seas.upenn.edu/~halasz/ICRA07SwarmBermanetal.pdf>
- [19] Marco Dorigo and Gianni Di Caro, The Ant Colony Optimization Meta-Heuristic, 1999.
- [20] Xiaoyuan Luo, Shaobao Li, and Xinping Guan, "Flocking Algorithm with Multi-Target Tracking for Multi-Agent Systems," Pattern Recogn. Lett., vol. 31, no. 9, pp. 800-805, July 2010. [Online]. <http://dx.doi.org/10.1016/j.patrec.2010.01.014>
- [21] Andrew Davison, Killer Game Programming in Java.: O'Reilly Media, Inc., 2005.
- [22] Feng WeiXing, Wang KeJun, Ye XiuFen, and Guo ShuXiang, "Novel Algorithms for Coordination of Underwater Swarm Robotics," in Mechatronics and Automation, Proceedings of the 2006 IEEE International Conference on, 2006, pp. 654-659.
- [23] Guy Theraulaz, Swarm Intelligence. Oxford: Oxford University Press, 1999.
- [24] A F T Winfield and Julien Nembrini, "Safety in Numbers: Fault Tolerance in Robot Swarms," International Journal on Modelling Identification and Control, vol. 1, no 1, pp. 30-37, 2006.
- [25] A. Yamashita, T. Arai, J. Ota, and H. Asama, "Motion Planning of Multiple Mobile Robots for Cooperative Manipulation and Transportation," Robotics and Automation, IEEE Transactions on, vol. 19, no. 2, pp. 223-237, 2003.
- [26] Alan F. T. Winfield, Christopher J. Harper, and Julien Nembrini, "Towards Dependable Swarms and a New Discipline of Swarm Engineering," in Proceedings of the 2004 International Conference on Swarm Robotics. Berlin, Heidelberg: Springer-Verlag, 2005, pp. 126-142. [Online]. http://dx.doi.org/10.1007/978-3-540-30552-1_11
- [27] Erol Sahin, Sertan Girgin, Levent Bayindir, and Ali Emre Turgut, "Swarm Robotics," in Swarm Intelligence: Introduction and Applications, Christian Blum and Daniel Merkle, Eds.: Springer, 2008, pp. 87-100.
- [28] Lynne E. Parker, "ALLIANCE: An Architecture for Fault Tolerant Multi-Robot Cooperation," IEEE Transactions on Robotics and Automation, vol. 14, pp. 220-240, 1998.
- [29] Kai Jin, Ping Liang, and Gerardo Beni, "Stability of Synchronized Distributed Control of

- Discrete Swarm Structures.," in ICRA, 1994, pp. 1033-1038. [Online]. <http://dblp.uni-trier.de/db/conf/icra/icra1994-2.html#JinLB94>
- [30] Toshio Fukuda, Daisuke Funato, Kousuke Sekiyama, and Fumihito Arai, "Evaluation on Flexibility of Swarm Intelligent System.," in ICRA, 1998, pp. 3210-3215. [Online]. <http://dblp.uni-trier.de/db/conf/icra/icra1998-4.html#FukudaFSA98>
- [31] M.C. De Gennaro and A. Jadbabaie, "Formation Control for a Cooperative Multi-Agent System Using Decentralized Navigation Functions," in American Control Conference, 2006, 2006, pp. 6
- [32] S. Nouyan, R. Gross, M. Bonani, F. Mondada, and M. Dorigo, "Teamwork in Self-Organized Robot Colonies," *Evolutionary Computation, IEEE Transactions on*, vol. 13, no. 4, pp. 695-711, 2009.
- [33] Wei-Min Shen, Peter Will, Aram Galstyan, and Cheng-Ming Chuong, "Hormone-Inspired Self-Organization and Distributed Control of Robotic Swarms," *Autonomous Robots*, vol. 17, no. 1, pp. 93-105, #jul# 2004.
- [34] M. Gerla, Y. Yi, Kaixin Xu, and Xiaoyan Hong, "Team Communications Among Airborne Swarms," in *Aerospace Conference*, 2003. Proceedings. 2003 IEEE, vol. 3, 2003, pp. 1303-1312.
- [35] A.H. Purnamadajaja and R. Andrew Russell, "Pheromone Communication: Implementation of Necrophoric Bee Behaviour in a Robot Swarm," in *Robotics, Automation and Mechatronics*, 2004 IEEE Conference on, vol. 2, 2004, pp. 638-643 vol.2.
- [36] Yuan-Shun Dai, M. Hinchey, M. Madhusoodan, J.L. Rash, and Xukai Zou, "A Prototype Model for Self-Healing and Self-Reproduction In Swarm Robotics System," in *Dependable, Autonomic and Secure Computing*, 2nd IEEE International Symposium on, 2006, pp. 3-10.
- [37] Eric Chapman and Ferat Sahin, "Application of Swarm Intelligence to the Mine Detection Problem," in *SMC* (6), 2004, pp. 5429-5434.
- [38] V. Kumar M and F. Sahin, "A Swarm Intelligence Based Approach to the Mine Detection Problem," in *Systems, Man and Cybernetics*, 2002 IEEE International Conference on, vol. 3, 2002, pp. 6 pp. vol.3.
- [39] Vignesh Kumar Munirajan and Ferat Sahin, "Cognitive Maps in Swarm Robots for the Mine Detection Application," in *SMC*, 2003, pp. 3364-3369.
- [40] Yong Chye Tan and B.E. Bishop, "Evaluation of Robot Swarm Control Methods for Underwater Mine Countermeasures," in *System Theory*, 2004. Proceedings of the Thirty-Sixth Southeastern Symposium on, 2004, pp. 294-298.
- [41] S. H M Amin and A. Adriansyah, "Particle Swarm Fuzzy Controller for Behavior-based Mobile Robot," in *Control, Automation, Robotics and Vision*, 2006. ICARCV '06. 9th International Conference on, 2006, pp. 1-6.
- [42] William M. Spears, Diana F. Spears, Jerry C. Hamann, and Rodney Heil, "Distributed, Physics-Based Control of Swarms of Vehicles," *Auton. Robots*, vol. 17, no. 2-3, pp. 137-162, Sept 2004. [Online]. <http://dx.doi.org/10.1023/B:AURO.0000033970.96785.f2> <http://dx.doi.org/10.1023/B:AURO.0000033970.96785.f2>
- [43] Craig W. Murray, Kevin Johnston e Colin R. McInnes Mohamed H. Mabrouk, "Internal Agent States: Experiments Using the Swarm Leader Concept," in *Towards Autonomous Robotic Systems (TAROS 08)*, 2008.
- [44] Fiona Higgins, Allan Tomlinson, and Keith M. Martin, "Survey on Security Challenges for Swarm Robotics," in *Proceedings of the 2009 Fifth International Conference on Autonomic and Autonomous Systems*, Washington, DC, USA, 2009, pp. 307-312. [Online]. <http://dx.doi.org/10.1109/ICAS.2009.62>
- [45] Jongeun Choi, Joonho Lee, and Songhwai Oh, "Swarm Intelligence for Achieving the Global Maximum Using Spatio-Temporal Gaussian Processes," in *American Control Conference*, 2008, 2008, pp. 135-140.
- [46] Poul E. Heegaard and Otto J. Wittner, "Self-Tuned Refresh Rate in a Swarm Intelligence Path Management System," pp. 148-162, 2006. [Online]. http://dx.doi.org/10.1007/11822035_13
- [47] C. Johnson, G.K. Venayagamoorthy, and P. Palangpour, "Hardware Implementations of Swarming Intelligence - A Survey," in *Swarm Intelligence Symposium*, 2008. SIS 2008. IEEE, 2008, pp. 1-9.

[48] Y. Liu and K. M. Passino, "Swarm Intelligence: Literature Overview," tech. rep., Ohio State University, March 2000.

[49] F. Sahin, "Groundscouts: Architecture for a Modular Micro Robotic Platform for Swarm Intelligence and Cooperative Robotics," in Systems, Man and Cybernetics, 2004 IEEE International Conference on, vol. 1, 2004, pp. 929-934 vol.1.

[50] Anders Lyhne Christensen, Rehan O'Grady, and Marco Dorigo, "From Fireflies to Fault-Tolerant Swarms of Robots," Trans. Evol. Comp, vol. 13, no. 4, pp. 754-766, #aug# 2009. [Online]. <http://dx.doi.org/10.1109/TEVC.2009.2017516>

*32nd Digital Avionics Systems Conference
October 6-10, 2013*